REMARKS

Claim 6 is pending. Claim 6 is rejected.

In the Office Action dated June 23, 2008, claim 6 is objected to for an informality and is also rejected under 35 U.S.C. §103(a) as being unpatentable over Mishra et al. "Security Services Markup Language" ("Mishra") in view of U.S. Patent No. 6,226,752 to Gupta et al. ("Gupta").

Independent claim 6 has been amended delete the phrase "operable to" and to recite that the ASP pulls authentication information from an aggregator using tokens that have been presented by the client to the ASP. Support for this amendment can be found in paragraph [0058] of the specification.

Applicants' invention relates to a method for providing a single-sign-on mechanism within an ASP aggregator service. Independent claim 6 recites the limitation of an aggregator token that is generated by an ASP aggregator service and sent to a client device after its user has been successfully authenticated during a single-sign-on operation that is provided by the ASP aggregator service. The aggregator token then accompanies any request from the client to aggregated applications within the ASP aggregator service's infrastructure. In the embodiment of the invention recited in independent claim 6, the aggregator token comprises an indication of an address or resource identifier within the ASP aggregator service to which a client/user can be redirected when the client/user needs to be authenticated by the ASP aggregator service.

Examiner states that Mishra does not disclose that the ASP is operable to pull authentication information from an aggregator using tokens that have been presented by the client to the ASP. Applicants agree with Examiner on this point. More specifically, the ASP disclosed in Mishra would not necessarily know which aggregator performed the authentication of the client and subsequently generated the token presented by the client to the ASP. As an example, it is common for an aggregator to provide single sign-on services to an aggregate group of individual ASPs. In fact, the only commonality the individual ASPs may share is the aggregator. Likewise, an individual ASP may be aggregated with other individual ASPs by a plurality of aggregators. In such a case, the ASP has no foreknowledge of which aggregator authenticated the client, hence the need to pull authentication information from the corresponding aggregator that issued the token that is to the ASP by the client.

On pages 5-6, Examiner states:

However, Mishra does not teach what the ASP (i.e., Site B) and the ASP aggregator service (i.e., Site A) do if it is determined that the user has not been properly authenticated (i.e., the aggregator token is expired). Specifically, Mishra does not disclose: (i) the logon resource identifier is the URL of a login Web page, (ii) determining that the request was not accompanied with a valid application authentication token, (iii) determining that the client of a user of the client has not been properly authenticated; and (iv) sending to the client a response indicating the logon resource identifier as a redirectable location.

Similar to Mishra, Gupta discloses a method for accessing a resource at an ASP (i.e., an application server) protected by a login server, which provides aggregator tokens for accessing the ASP (i.e., the login server authenticates a user and provides the user with a cookie, the user submits the cookie together with a request to access the application server) (fig. 2; Abstract; col. 11, lines 10-38). In addition, Gupta discloses that if the ASP determines that a user has not been properly authenticated (i.e., the cookie accompanying the request has expired), the ASP will send to the client a response indicating a URL of a login Web page, which is implemented as a default Web page of the login server, as a destination.

Applicants respectfully submit that the combination of Mishra and Gupta fails to provide all of the limitations recited in independent claim 6. Applicants concur with Examiner that Gupta teaches the redirection of a client to a URL of a login Web page (col. 12, lines 13-16). However, Gupta presumes that the ASP has foreknowledge of the URL of a login Web page used to authenticate the client. Furthermore, Gupta fails to teach how the ASP acquires the URL of a login Web page for a redirect operation. More specifically, while Gupta may teach the redirection of a client to a URL of a login Web page, the URL (the logon resource identifier) is not provided by the cookie (the aggregator token).

Applicants respectfully submit that the combination of prior art references cited by Examiner do not disclose the combination of features cited in independent claim 6, as amended. For the reasons set forth above, therefore, Applicants respectfully submit that the rejection of independent claim 6 under 35 U.S.C. §103 has been overcome and this claim should be passed to allowance.

CONCLUSION

In view of the amendments and remarks set forth herein, the application is believed to be in condition for allowance and a notice to that effect is solicited. Nonetheless, should any issues remain that might be subject to resolution through a telephonic interview, the examiner is requested to telephone the undersigned at 512-338-9100.

CERTIFICATE OF TRANSMISSION

I hereby certify that on October 23, 2008 this correspondence is being transmitted via the U.S. Patent & Trademark Office's electronic filing system.

/Gary W. Hamilton/

Respectfully submitted,

/Gary W. Hamilton/

Gary W. Hamilton
Attorney for Applicant(s)
Reg. No. 31,834